

The BioSig™ Revolution

**“A lie can travel half way around the world while the truth is putting on its shoes.”
– Mark Twain**

Our dependence upon electronic techniques for creating and distributing documents, and conducting transactions of all types, is immense—and growing. We send and receive more information via email than we do through the postal service. We order billions of dollars of goods and services online. And we are under increased pressure, both financial and regulatory, to convert paper-based processes to electronic ones.

But how safe are our electronic transactions? When you transmit a confidential bid, can you be sure that it won't be intercepted? When you receive an emailed document, can you be sure that it was actually sent by the person on the “From” line? How can you be confident that the timesheet your employee filed electronically was never altered? We could keep asking questions like these, but we'd rather talk about the answer.

For Superior Data Security, Just Sign Here: with BioSig™

BioSig™ is a remarkable technology capable of addressing some of today's most serious information security and integrity issues. BioSig™ is an authenticating technology, a tool for positively determining whether a person is—or is not—who he or she claims to be. It has applications across a wide range of industries, and can be used in a multitude of different ways. BioSig™ works with inexpensive, off-the-shelf hardware to compare a person's signature with a

“Unlike fingerprints, retinal or DNA patterns which remain constant over time, the execution of a person's signature will be unique and individual at that particular moment. Handwriting remains one of the most powerful human identifiers that exist today.”

**-Marc Gaudreau, Forensic Sciences
Laboratory Manager, Canada
Customs and Revenue Agency**

reference file (or “model”). The process is fast, reliable, and exceptionally simple. There is nothing for the user to remember: they simply sign their own name on an electronic pad, on paper with an electronic pen, or on a handheld computer screen, and BioSig™ does the rest.

The software is exceptionally sophisticated. Developed originally by Bell Labs for Lucent Technologies, BioSig™ is true biometric security. It does not work by comparing the appearance of a signature with the model; a modestly-talented forger could easily defeat such a system. Instead, it takes dozens of different measurements of the

way in which the signature is entered to generate a file which is unique to the user. This makes BioSig™ a true behavioral biometric: there may be thousands of “John Smiths” in the world, but no two of them sign their name the same way.

“Cracking” biometric security measures is the stuff of movies: we've seen our heroes fool retinal scanners with clever contact lenses, or fingerprint readers with molds taken from other peoples' fingers. But there is no obvious way to fool BioSig™. A signature file cannot be intercepted and re-used, because the software knows that nobody signs their name quite the same way every

time—a perfect duplicate of a previously submitted signature is always rejected. The signature file includes an embedded time stamp, so that suspiciously old signatures can also be rejected. And since the file is utterly unintelligible if intercepted (it cannot be used to infer what the signature looked like, nor can it be modified in a way that evades the “no duplicates” rule), it can even be used safely in settings where transmission of the signature file is not entirely secure.

As with all biometrics, users need to be enrolled in the system to generate a signature model. This can be accomplished either through a dedicated enrollment (or “training”) session, where the user signs three to six times in succession (depending on the level of accuracy required by the application), or on a rolling basis—as the user signs their name in the ordinary course of business, a model is generated from the series of signatures. The model can be set to adapt over time to the almost imperceptible changes we make to our signatures.

BioSig™ has many applications. It can be used across a range of industries for access control (in lieu of a password or code number, for restricting access to networks or even buildings); to “lock down” documents and records, and prevent them from being altered (the digital signature can be “bound” to the document, so that the document carries its own proof of authorship and cannot be modified); and to meet “electronic signature” requirements under numerous state and federal laws and regulations while meeting real-world requirements for reliable, low-cost, user-friendly data security.

The Benefits of BioSig™

BioSig™ has numerous advantages over other approaches to signature verification, and other forms of data security, in many applications.

Market-Based Advantages

- **Low hardware costs and flexible hardware requirements:** BioSig™ works well with many different kinds of devices already in widespread use, including notebook computer touch pads, handheld computers, the tablet-based computers, and point-of-sale signature capture pads. It could also be used with stylus-enabled cell phones or other “convergence devices.”
- **Low administrative costs:** Signatures are not forgotten as passwords and PINs are, nor do they need to be changed routinely to thwart detection. Business costs for users may also be reduced, not only through fraud reduction, but also by replacing time-consuming visual signature comparison with automated verification in applications such as point-of-sale check cashing.
- **Durability:** Digital pads are rugged and virtually indestructible when compared to the cameras and sensors that enable other biometric technologies.

“I would say today that the weakest link in security management is that passwords are used to identify who is running the system.”

-Bill Gates

Technological Advantages

- **High Security:** BioSig™ technology consistently and accurately distinguishes authentic signatures from forgeries. It is highly reliable and offers enhanced security in many situations where none currently exists.
- **Robustness:** BioSig™ captures information about the process of signing a name, rather than the appearance of the signature, making it all but impossible to trick the system through forgery. The model signature used by BioSig™ for reference (and the file

- transmitted during verification) contains no information about the appearance of the signature, or other intelligible information. And unlike an ID card or other “token,” a signature is not a physical object that can be stolen or left at home by its owner.
- **Portability:** The model file is exceptionally small, and can be located in a central database, a portable or handheld computer, or embedded in a smart card or magnetic stripe card (such as a credit card stripe). The attachment of a signature to a document (“signature binding”) works with any type or file format of document, and adds almost nothing to the size of the document.
 - **Flexibility and Customization:** This technology can be used to verify a signature, initials, or even a password selected by the user. Risk tolerance can readily be adjusted, to minimize either false positives or false negatives, as business requirements dictate.

Behavioral Advantages

- **User-friendliness:** Unlike most other biometrics (such as fingerprint, hand, iris, or facial scanning), BioSig™ requires no change to user behavior, and is not seen as intrusive—many of the leading applications for BioSig™ are those where the user is already signing their name, and the only change is the use of a stylus instead of a pen.

Legal Advantages

- **Enforceability:** BioSig™ can be readily incorporated into applications that meet the requirements of numerous statutes and regulations, including the Electronic Signatures in Global and National Commerce Act (E-SIGN), Uniform Electronic Transaction Act (UETA), Health Insurance Portability and Accountability Act (HIPAA), 21 CFR Part 11, and others. Indeed, an application incorporating BioSig™ can generate such strong evidence of authorship, intent to be bound, and document integrity, as to lower the risk of dispute and the cost of dispute resolution. BioSig™ is also an outstanding tool for generating an enforceable audit trail for protecting intellectual property (e.g., when used for signing electronic lab notebooks in which patentable discoveries are described).

The advantages can be summarized as follows:

	BioSig	Finger Scanning/ Other Biometrics	Password	Card or “Token”
Low hardware costs	★	☒	★	☒
Versatile hardware (used for other purposes)	★	☒	★	☒
Multiple hardware vendors	★	☒	★	☒
Durable hardware	★	☒	★	★
Low administrative costs	★	(varies)	☒	☒
Hard to crack	★	★	☒	★
Can’t be lost or stolen	★	★	☒	☒
Can’t be forgotten	★	★	☒	☒
User-friendly	★	(varies)	☒	☒
Consistent with existing business practices	★	☒	★	☒

About The Technology

The core of BioSig™ is a set of patented, complex algorithms created by Bell Labs for Lucent Technologies. The major patents in the package are:

US 5,828,772: Method and apparatus for parametric signature verification using global features and stroke-direction codes

Signature verification techniques developed by other companies make use of so-called “global” features describing general characteristic of a signature, such as total time to sign. This patent secures the use of a combination of both “global” features of a signature, and “local” signature curve matching, to verify the authenticity of the signer. This technique provides for higher verification accuracy than reliance on global features alone.

US 5,898,156: Validation stamps for electronic signatures

This patent allows VII to engage not only in any signature verification business (as per patent 5,828,772), but also in the business of verifying the authenticity of electronic documents. The combination of these two technologies is critical for any document-oriented applications. Patent 5,898,156 describes a method of verifying that a given handwritten electronic signature was intended for the given electronic document. The technology covered in the patent prevents such forms of deception as the attachment of an authentic signature from one document to a different document. The patent also thwarts any attempt to fraudulently re-generate a handwritten signature and attach it to another document by re-constructing the timing information in a signature from its geometric shape as sampled by a tablet digitizer. It is oftentimes important to display a signature shape on an unencrypted portion of a document to visually present the signature to a user. However, such an image can present a security threat. The patent covers the entire concept of modifying the geometric characteristics of a signature to hide the signature stroke pattern and speed while preserving the shape of the signature.

Contact Us

The BioSig™ technology package is available for license, to be incorporated into your applications. Call us to see a demo, and to discuss pricing and other terms.

Joel E. Simkins
Chief Marketing Officer
Vector Intelligence, Inc.
604 S. Washington Sq. #1003
Philadelphia, PA 19106

(215) 923-5942
jsimkins99@earthlink.net